REMARKS

Claim Status

Claims 1-33 are now pending, with claims 1, 32 and 33 being the only independent claims. Claims 1-33 have been amended. The amendments to claims 2-31 are merely cosmetic or clarifying in nature. Support for the amendments to the independent claims may be found, for example, at pg. 5, lines 3-9, at pg. 8, line 34 thru pg. 9, line 3, and at pg. 12, line 37 thru pg. 13, line 6 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claim 3 has been objected to based on a minor informality. Withdrawal of this objection is now in order, as explained below.

Claims 1-31 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Publication No. 2002/0129247 ("*Jablon*") in view of U.S. Patent No. 5,867,577 ("*Patarin*").

Claim 32 stands rejected under 35 U.S.C. §103(a) as unpatentable over *Jablon* in view of *Patarin*, and further in view of U.S. Publication No. 2003/0182554 ("*Gentry*").

Applicants note that claim 33 is also pending in this Application. However, the Examiner has failed to consider claim 33. An indication that independent claim 33 has been considered, and its status, is therefore requested.

Applicants have carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, Applicants respectfully assert that all claims now presented for examination in the present application are patentable over the cited art.

Amendments Addressing Formalities

The Examiner has stated that "[c]laim 3 recites ... secrete...". In response to this objection, applicants have amended claim 3 in a self-explanatory manner. Withdrawal of this objection to claim 3 is deemed appropriate.

Descriptive Summary of the Prior Art

Jablon discloses "methods and apparatus for securely proving knowledge of a shared small secret password between two parties using messages exchanged across an open communication channel" (see paragraph [0004]).

Patarin discloses "a method for authenticating a data carrier or a device as genuinely issued by an authorized organization" (see col. 1, lines 9-11).

Gentry discloses the determination and use of a shared secret in an identity-based cryptosystem for encoding and decoding communications between two entities without the disadvantages associated with key escrow (see paragraph [0002]).

Summary of the Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

The specification discloses an asymmetrical cryptographic method that is partially implemented by a hard-wired electronic chip which is configured to protect it against fraud in transactions with an application. This protection is achieved when the electronic chip calculates

an authentication value V from input parameters that are provided to the chip, and the application then verifies the calculated authentication value.

A parameter x is calculated by the application and stored in a data memory of the electronic chip prior to sale of the electronic chip. The authentication value V is calculated when the chip sends the stored parameter x to the application for a particular transaction, where the parameter x is first calculated at the chip using a mathematical function whose input parameters include a random number r which is generated at the chip. On each authentication, the electronic chip recalculates this random number, calculates a corresponding x, compares the calculated x to the stored x, and then transmits the stored value of the parameter x in the data memory of the chip to the application if the comparison is successful.

The electronic chip also calculates a parameter y which is a calculated based on a serial function applied to the chip-calculated random number r and a private key s. The electronic chip sends to the application the calculated authentication value V, which is comprised of the parameter y. The application then calculates the value y using a function whose input parameters are the transmitted value x and public parameters which include a public key p. Consequently, the claimed invention implements the calculation of an authentication value y by a hard-wired electronic chip which is verified based on public parameters. As a result, the claimed invention achieves the integration of an active public key authentication mechanism into a low cost, hard-wired electronic chip.

Patentability of the Independent Claims Under 35 U.S.C. §103(a)

Independent claim 1 has been amended to recite, *inter alia*, producing a pseudo-random number r at the application prior to a transaction; calculating a corresponding parameter x at the application prior to the transaction, said parameter x being linked to the pseudo-random number r by

a mathematical relationship; storing the parameter x in a data memory of the electronic chip prior to the transaction; producing, at the chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the chip, said chip reading the stored parameter x calculated by the application prior to the transaction...". Independent claims 32 and 33 have also been amended to include limitations directed to defining that the electronic chip reads a parameter calculated by the application prior to the transaction, where the parameter is linked to a pseudo-random number by a mathematical relationship and is stored in a data memory of the chip. Thus, each of independent claims 1, 32 and 33 have been amended to clarify that a parameter is calculated by the application and stored in the electronic chip prior to the performance of a transaction. Support for this claimed feature may be found, for example, at pg. 12, line 37 thru pg. 13, line 6 of the specification as originally filed. No new matter has been added.

The Examiner (at pg. 2 of the Office Action) asserts that:

> Jablon discloses the producing random number specific to transaction see Fig. 1 item 103; sending of parameter x, that is linked to random number r by a mathematical relationship see Fig. 1 item Q_A; calculating a parameter y whose parameters are random number r specific to transaction and private key s see Fig. 1 item 105 & 107; sending the authentication value see item 108; verifying the authentication using public key see item 127.

Applicants respectfully disagree that *Jablon* either teaches or suggests applicants' claimed method as recited in now-amended independent claim 1.

Jablon relates to a method for authenticating one party to the other using a series of messages that are exchanged over an open, insecure network, where interception or modification of the messages by an un-trusted third party may be possible (see Abstract). *Jablon* (paragraph [0040]) describes the establishment of "a large mutually-authenticated shared secret key between parties over an open insecure channel, where the authentication is based solely on mutual possession of a potentially small shared secret, such as a password".

As described at paragraph [0057] of *Jablon*, a pair of entities, i.e., Alice and Bob, "alone share knowledge of a secret password S". Bob proves his identity to Alice by proving his knowledge of the result of a key exchange protocol, which is determined by parameters set according to a function of S". This exchange is known in the art as a simple password-authenticated exponential key exchange (SPIKE).

In contrast, the claimed invention is directed to an asymmetrical cryptographic method for protecting a hard-wired electronic logic chip against fraud in transactions between the electronic chip and an application. Consequently, the claimed invention provides an asymmetrical pair of keys comprised of a private key s and a public key p. In addition, performance of the calculation of an authentication value V occurs within the electronic chip using input parameters that include a random number r. *Jablon* fails to teach or suggest the claimed invention.

For example, *Jablon* fails to teach or suggest that a parameter is calculated by the application and stored in the electronic chip prior to the performance of a transaction. With reference to Fig. 1 of *Jablon,* even assuming, *arguendo*, that Q_A corresponds to parameter x recited in independent claim 1 that would be sent to Bob, where $Q_A=H_{RA}(g)$, *Jablon* would still fail to teach or suggest applicants' claimed invention as recited in now-amended independent claim 1. Independent claim 1 recites the steps of "producing a pseudo-random number r at the application prior to a transaction; calculating a corresponding parameter x at the application prior to the transaction, said parameter x being linked to the pseudo-random number r by a mathematical relationship; storing the parameter x in a data memory of the electronic chip prior to the transactions". Consequently, now-amended independent claim 1 defines that a parameter x is calculated by the application and stored in a data memory of the electronic chip, all prior to a transaction. Clearly, *Jablon* does not teach the recitations of amended claim 1.

Jablon (paragraph [0066]; Fig. 1) teaches that Q_A is computed by Alice at step 104, which is part of a sequence comprised of steps 103, 104 and 106, where the computed Q_A is then sent to Bob. *Jablon* thus teaches that Q_A is not calculated by Bob prior to the transaction and, consequently, there is no previous or earlier or pre-transaction calculation corresponding to parameter x which could have been stored in any internal memory of Alice. Moreover, *Jablon* (paragraph [0101]) explains that the order of the messages Q_A and Q_B may change, where Q_A "may be sent to Bob either before, after, or at the same time as Q_B is sent to Alice". However, this does not mean that Q_A is sent prior to step 102 or step 103 (see Fig. 1 of *Jablon*) but, rather, only that the temporal order of Q_A and Q_B in relationship to each other may change. *Jablon* fails to teach or suggest now amended independent claim 1 for at least this initial reason.

Independent claim 1 further recites the step of "producing, at the chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the chip". *Jablon* also fails to teach or suggest this limitation. Independent claim 1 recites that the pseudo-random generator is "included in the chip". In *Jablon*, however, the value of the random number R_A is chosen from between 1 and N, and N is actually known by Bob. Moreover, *Jablon* clearly teaches that the random number calculated at Bob is R_B, which differs from R_A. *Jablon* thus fails to teach or suggest now-amended claim 1.

Independent claim 1 further defines that the authentication value is entirely or partly equal to the result of a serial function whose input parameters are at least the random number r and a private key s. *Jablon*, in contrast, teaches that the verification value V_A is constructed as the result of a one-way function of K, which is itself the result of a function whose input parameter is Q_B that is computed by Bob and sent to Alice from Bob (see paragraph [0076]). *Jablon* thus fails to teach or suggest now-amended claim 1.

Moreover, independent method claim 1 recites the step of "verifying, at the application, said authentication value V via a verification function whose input parameters consist of public parameters including at least a public key p". *Jablon* fails to teach or suggest this claimed step. As recited in claim 1, the input parameters of the verification function are public parameters. *Jablon*, on the other hand, teaches that the input parameter of verification function h(h) is K (see FIG. 1, 109 & 129), i.e., the input parameter is secret and known only to Alice and Bob (where K can then be transformed into a secure authenticated session key). *Jablon* thus fails to teach or suggest now-amended independent method claim 1 for at least this additional reason.

The Examiner cites *Patarin* in an effort to cure the shortcomings of *Jablon*, i.e., the failure to teach or suggest "a chip and an application conducting the said authentication". However, the combination of *Jablon* and *Patarin* fails to achieve the claimed invention, at least because (as discussed above) *Patarin* also fails to teach or suggest that a parameter x is previously calculated by the application and stored in a data memory of the electronic chip, all prior to the transaction, as recited in now-amended independent claim 1.

Patarin relates to the authentication of a data carrier that is intended for enabling a transaction or access to a service or a location. *Patarin* (col. 1, lines 25-35) explains that the "object of the invention is to propose a method of this type which employs the simplest possible means in the carrier itself and in an optional terminal of the distributor that is intended to cooperate with the carrier. In the case where the carrier is electronic, for example, it is desirable for it to be made up solely of a memory, without any associated calculation circuits, and for each memory to have the smallest possible size." However, the skilled person would have no reason to even consider the teachings of *Patarin* were that person seeking, *arguendo*, to modify the structure of *Jablon* to achieve the method of independent claim 1.

Jablon describes methods for "two parties to use a small shared secret (S) to mutually authenticate one another over an insecure network" (see Abstract). *Patarin* specifically states that "[i]t is also desirable for neither the carrier nor the associated terminal to contain a secret key, because such a secret key is vulnerable to being discovered by someone with an intent to commit fraud" (see col. 1, lines 32-35). *Patrin* thus clearly teaches away from including a secret key in an electronic chip. Consequently, the skilled person would have no reason whatsoever to apply the disclosed EEPROM or other teachings of *Patrin* to the method of *Jablon*, absent impermissible hindsight analysis based on applicants' disclosure. Absent an electronic chip in which to store the parameter x that is calculated by the application prior to the transaction and stored in a data memory of an electronic chip, prior to the transaction, the deficiency of *Jablon* is apparent.

Furthermore, independent claim 1 explicitly recites the step of "calculating, at the chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function whose input parameters are at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys". *Patarin* fails to teach or suggest this step, because the card in *Patarin* does not perform any mathematical calculations since it is merely comprised of memory (i.e., EEPROM 2).

Independent claim 1 is therefore not rendered obvious and unpatentable by the proffered combination of *Jablon* and *Patarin*. Reconsideration and withdrawal of the rejection of claim 1 as unpatentable over the combination of *Jablon* with *Patarin* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

Independent Claim 32

The Examiner additionally cites *Gentry* in an effort to cure the shortcomings of *Jablon* and *Patarin*, i.e., the failure to teach or suggest "the use of public parameters exclusively to verify the authentication results", as recited in independent claim 32. *Gentry* relates to an authenticated ID-based cryptosystem including key agreement protocols that do not require key escrow. However, the combination of *Jablon*, *Patarin* and *Gentry* fails to achieve the claimed invention, at least because (as discussed above) *Gentry* also fails to teach or suggest a parameter x that is previously calculated by the application and stored in a memory means of an electronic chip, all prior to any transaction. For at least this reason, the recitations of independent claim 32 are not rendered obvious by *Gentry* in combination with *Jablon* and/or *Patarin*.

Applicants accordingly assert that amended independent claim 32 is patentable over the cited references, individually or in combination. Reconsideration and withdrawal of the rejection of claim 32 under 35 U.S.C. §103 are requested.

Dependent Claims

In view of the patentability of independent claims 1, 32 and 33, and for at least the reasons presented above, each of dependent claims 2-31 is believed to be patentable therewith over the prior art. Each of dependent claims 2-31 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: November 28, 2007